12.11.99 H PROV

Please type a plus sign (+) inside this box ⟶ +

Docket Number:	700-198P

PROVISIONAL APPLICATION FOR PATENT COVER SHEET (Small Entity)

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

INVENTOR(S)/APPLICANT(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Scott	Krueger	915 17th Avenue, Seattle, WA 98122
Daniel	Goodman	16750 NE 10th Avenue, N. Miami Beach, FL 33162

□ *Additional inventors are being named on page 2 attached hereto*

TITLE OF THE INVENTION (280 characters max)

SECURE NETWORKED TRANSACTION SYSTEM

CORRESPONDENCE ADDRESS

Direct all correspondence to:

□ Customer Number ______ ⟶ *Place Customer Number Bar Code Label here*

OR

☒ Firm *or* Individual Name	Anthony R. Barkume				
Address	Greenberg Traugrig				
Address	Met Life Building, 200 Park Avenue				
City	New York	State	NY	ZIP	10166
Country	USA	Telephone	212-801-9294	Fax	212-801-6400

ENCLOSED APPLICATION PARTS *(check all that apply)*

X	Specification	*Number of Pages*	17	☒	Small Entity Statement
X	Drawing(s)	*Number of Sheets*	5	☒	Other (specify) ASSIGNMENT

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

		FILING FEE AMOUNT ($)
☒	A check or money order is enclosed to cover the filing fees	
□	The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: ______	$75.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

□ Yes, the name of the U.S. Government agency and the Government contract number are: ______

Respectfully submitted,

SIGNATURE ______ Date December ~~15~~ 16 ARB, 1999

TYPED or PRINTED NAME Anthony R. Barkume REGISTRATION NO. *(if appropriate)* 33,831

TELEPHONE 212-801-9294

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

Page 1 of 2

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) AND 1.27 (c)) - SMALL BUSINESS CONCERN	Docket No. 700-198P

Serial No.	Filing Date	Patent No.	Issue Date
Unkoown	Herewith	N/A	N/A

Applicant/
Patentee: KRUEGER et al.

Invention: SECURE NETWORKED TRANSACTION SYSTEM

I hereby declare that I am:

☐ the owner of the small business concern identified below:

☒ an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN: Debit.net, Inc.

ADDRESS OF CONCERN: 16750 NE 10th Avenue, North Miami Beach, Florida 33162

I hereby declare that the above-identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the above identified invention described in:

☒ the specification filed herewith with title as listed above.

☐ the application identified above.

☐ the patent identified above.

If the rights held by the above-identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed on the next page and no rights to the invention are held by any person, other than the inventor, who could not qualify as an independent inventor under 37 CFR 1.9(c) or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

☒ no such person, concern or organization exists.
□ each such person, concern or organization is listed below.

FULL NAME ________________
ADDRESS ________________
□ Individual □ Small Business Concern □ Nonprofit Organization

FULL NAME ________________
ADDRESS ________________
□ Individual □ Small Business Concern □ Nonprofit Organization

FULL NAME ________________
ADDRESS ________________
□ Individual □ Small Business Concern □ Nonprofit Organization

FULL NAME ________________
ADDRESS ________________
□ Individual □ Small Business Concern □ Nonprofit Organization

Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING: Daniel Goodman
TITLE OF PERSON SIGNING
OTHER THAN OWNER: President
ADDRESS OF PERSON SIGNING: 16750 NE 10th Avenue, North Miami Beach, Florida 33162

SIGNATURE: ________________ DATE: December 15, 1999

Docket No. 700-198P

UNITED STATES PROVISIONAL PATENT APPLICATION

OF: SCOTT KRUEGER
DANIEL GOODMAN

FOR: SECURE NETWORKED TRANSACTION SYSTEM

BACKGROUND OF THE INVENTION

The present invention relates to systems that allow debit cards, credit cards, Direct Check/ACH and other financial transaction instruments to be used in networked purchasing environments between a merchant, customer, and a third party processor. The third party processor acts as an intermediary or clearinghouse for transactions.

Debit cards such as those typically provided by financial institutions such as banks or credit unions require the card to be encoded or the system to be encoded to recognize the card / Personal Identification Number (PIN) combination. When used at an ATM or point of sale terminal, the system contacts the financial institution or a representative thereof with the user's account number and PIN number. The account is checked to determine whether sufficient funds exist for the purchase or cash request. The system records the parameters of the transaction to make the updates to the accounts such that the funds are transferred between parties of the transaction.

Prior art systems utilize various data encryption methods to secure the transmission of the customer's debit card/account number, customer's PIN number, the merchant's ID or code, to the various banking and transaction clearing systems that are checked at the point of sale such that an approval number is received by the merchant indicating that the transaction has been approved. The point-of-sale system or a separate card reader is used to connect directly to the clearing system.

While this type of transaction allows a user to directly pay for purchases at the point of sale, it allows the potential for an unscrupulous merchant, or a party intercepting communications to have access to the user's account number and PIN number.

In an e-commerce environment, the user accesses a merchants web site, indicates the items to be purchased and is requested to supply some means to pay for the items during the checkout process. The user typically enters the credit card number and the expiration date of the card to secure the credit transaction and shipping preferences. The merchant receives this information and generates a request that is transmitted to a credit clearing system that requests approval for the purchase and transfers back an approval code to the merchant. The merchant may at this point indicates to the customer that the purchase was successful and supplies an approval page to the customer.

Since the transaction occurs over the Internet, users have concerns over the privacy and security of the information entered. These privacy and security issues limit the amount of customers that use these forms of commerce at this time. Businesses have been trying to generate more robust security mechanisms to calm nervous customers, but these system still require the customer to provide the complete billing information to the merchant to complete the sale. Robust encryption processes help to reduce the customer's anxiety to some extent.

While credit cards are commonly used in point-of sale and on-line transactions, the merchant is charged a variable fee for the transaction by the credit authorization system based on the risk of the purchase. A higher rate for example, may be charged where the user is not at the point of sale, but is instead making the purchase at a remote location via a computer. The potential for fraud may be increased when the customer is not visible. Since the credit card company has power to act against unscrupulous merchants and to protect the consumer against fraud by merchants, customers are less concerned about the credit transaction that they would be regarding a debit transaction.

In contrast to credit purchases, there are no intermediaries to protect a customer when a debit transaction occurs. Debit transactions in contrast cause direct modifications to the clients bank account or financial assets held in a financial institution. The customer is vulnerable to direct funds transfer and withdrawal activity if someone performs these types of transactions without the customer's knowledge.

What is desired therefore is a system for allowing a customer to purchase items where the customer is not required to give the PIN number of the debit card to a merchant during an on-line purchase. It is another object of the present invention that the merchant or any party intercepting a communication between the customer and merchant, never has access to the customer's PIN number throughout the transaction. It is a further object of the present invention that all the information required to complete a transaction never exists in one transmission on the public network.

It is an object of the invention to provide a system where a third party trusted verification system is contacted during the purchase process by the merchant to request the processing of a customer's debit transaction where the merchant only knows the card number. The trusted verification system separately receives the PIN number from the customer and processes the transaction with the credit/debit processing system.

SUMMARY OF THE INVENTION

A customer at a customer computing device, interacting with a merchant's computer system/web site, decides to buy an item with a Debit/Check card. The merchant transmits details of the transaction to a trusted third party verification system including card number, merchant number, and transaction amount. The verification system returns a transaction ID and unique verification number to the merchant. The merchant redirects the customer to the verification system site, passing the transaction ID as part of the communications address. The verification system interacts with the user to acquire the PIN number for the debit/check card. Using the passed-in transaction ID and the acquired password (PIN), the verification system retrieves the merchant information from it's database, and provides the merchant number, card number, pin and transaction amount to the gateway of the Debit/Check card processing network. Upon retrieving a positive verification of the transaction success, the customer is redirected to the merchant site, passing the transaction ID and a unique verification as part of the redirection. The merchant's system compares the provided verification number against the expected verification number it had earlier received from the verification system. If they match, the merchant knows the transaction was successfully completed.

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 is a representation of the system components of the present invention;

Figure 2 is a representation of the front face of a debit card of the present invention;

Figure 3 a representation of the rear face of the debit card of the present invention;

Figure 4 is a process diagram of the method of the present invention;

Figure 5 is a representation of a prior art credit processing fields for on-line transactions;

Figure 6 is a representation of the debit card entry fields for on-line transactions of the present invention;

Figure 7 is a process step diagram of the present invention;

Figure 8 shows the icons associated with a sampling of the various debit processing network members that exist;

Figure 9 is a representation of an interface form for providing the PIN information that is delivered to a customer from the verification system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present system will be described with regard to Figure 1, for allowing a user to make purchases at a networked e-tailer or retail location using a debit card. In the preferred embodiment, the customer that wishes to purchase a product may access the web site of the merchant using a web enabled device such that the customer may access a purchasing interface provided by or for that merchant. The customer would typically use a desktop computer, set top box, or any other type of device capable of communications through a network. For example, a customer from a Pentium class computer with a display, keyboard, mouse and processor executing an operating system such as Windows CE, 95, 98, MAC O/S, or Linux or Unix with a communication connection to a network such as the Internet may execute a web browser such as Internet Explorer or Netscape to access the merchant's web site. Wireless and satellite communication devices may alternatively be used by the customer to communicate with the verification system and perform steps associated with completing the transactions associated with a purchase.

The customer computing device may alternatively be a device located at a retail location. For example, the user may use their debit card at the point of sale by swiping the card through a reader, then enter their PIN number on a separate system that is connected with the verification system of the present invention. The Internet-based verification step would be executed as a separate application having no direct connection to the merchant transaction. This would of course require a shift in the merchant's and customer's paradigm of their understanding of a point-of sale system. The separate components may be provided to allow the customer to establish a communication link to the verification system, where once connected, the customer may provide the remaining information to complete the transaction without communicating with the point of sale system.

The merchant computer means 20 may be a terminal connected to a network, point of sale system, or personal computer system, or server based system connected to a network that is capable of connecting to a merchant server web site. For Internet-based communications where a merchant web server is provided the server may comprise any networked computing devices capable of serving interface programs that customers may access to indicate desired purchases. The merchant computer means comprises communication means, storage means, and one or more processors to support the execution of the required processes. The merchant computer means may optionally have one or more monitors, and input devices such as keyboard, mouse, and mag-stripe reader. The mag-stripe reader is also known as a card-swipe reader, or card-swipe device.

The verification system therefore is a networked computer system that comprises communications means for receiving requests from merchants and for communicating with customers during the purchase process. The communication means also permits the verification system to communicate with debit card processing systems to process transactions for purchases. The verification system comprises memory means for retaining merchant records and customer records, and processor means for managing transactions.

The method of the present invention will now be described with regard to Figure 2. A customer at a customer computing device, interacting with a merchant's computer 20 system/web site, decides to buy an item with a Debit/Check card 40 at step 100. The merchant 20 transmits a request comprising details of the transaction to a trusted third party verification system (TVS) 30 at step 110, such as the customers card account number 42 (see Figure 2), merchant number (as determined from the merchant system) and transaction amount. The verification system 30 returns a transaction ID and unique verification number to the merchant 20 at step 120 that is associated with the merchant request. The merchant 20 redirects the customer's browser to the verification system 30 web site at steps 130 and 140. The redirect includes passing the transaction ID that was received from the verification system as part of the communications address (parameter of URL). The verification system receives the communication request from the customer and interacts with the customer at step 150 to acquire the PIN number for the debit/check card 40 at step 160. Using the passed-in transaction ID and the acquired password (PIN), the verification system retrieves the merchant information from it's database 32 at steps 162 and 164, and may optionally look up records for the customer in a customer database 34 at step 166, and provides the merchant number, card number, pin and transaction amount to the gateway of the Debit/Check card processing network 50 at step 170. Upon retrieving a positive verification of the transaction success at step 180, the customer is redirected to the merchant site at step 190, passing the transaction ID and a unique verification number as part of the redirection at step 200 back to the merchant.

Alternatively, the merchant's system may receive a separate notification message from the verification system 30 with the approved transaction ID and verification number. The merchant's system compares the provided verification number against the expected verification number it had earlier received from the verification system. If they match, the merchant knows the transaction was completed.

The method derives additional security because the merchants never have enough pieces of information to complete the transaction by themselves. The security of acquiring the PIN is enhanced because the network transmission containing the PIN never contains the corresponding card number and vice versa. Using readily available secure transmission protocols further increase security of all network transmissions.

This method is unique in that the merchant or any party intercepting a communication never has the customer's PIN number. It is further unique because the Debit/Check card and PIN numbers were never transmitted together during any part of the network exchanges between any of the three parties.

The debit card may be any type of debit card currently recognized by some of the present transaction service providers. The debit card typically has embossed characters 42 for the financial institution 43 and account number 44 where the characters are raised above the front of the card (see Figure 3) The most commonly quoted standards are the ISO/IEC 7810, 11, 12 and 13 series of standards. These standards are written for the credit and debit card market and so include information on the embossed characters on the cards as well as the track locations and information on the magnetic stripe that appears on the rear of the card 45. ISO/IEC 7811 has six parts with parts two and six specifically about low and high coercivity magnetic stripes. These standards include information on the magnetic properties that guarantee that the stripe can be read in a magnetic stripe reader in the U.S.A. as well as in Japan. The companion to the ISO/IEC 7811 series of standard is ISO/IEC 10 373. This document details the test methods for the ISO/IEC 7811 series of standards.

Debit cards are preferably processed by the verification system through the existing ATM backbone of service providers. There are several different ATM backbone networks, and many have reciprocity agreements, so one ATM can usually talk to the bank of another system. Some of the icons for the providers are displayed in Figure 8. A merchant that uses the functionality of the present system would typically be provided applets or modified HTML forms that direct the processing of debit transactions. For example, a modified form such as shown in Figure 6 would cause a transaction to be generated to contact the verification system through a first connection. Upon receiving the debit card information, the verification system may identify the appropriate ATM backbone to be contacted by interpreting the account number typed in by the customer and, or data read from the magnetic stripe of the debit card. A customer from a remote customer computer may be able to provide input to the merchant web page and the verification system using various hardware peripherals such as a mag-stripe reader or keyboard and mouse to enter the debit card number. If the customer is at a merchant location or on the merchants web site, the merchant or customer may select or choose the symbol of one of the ATM backbones indicated on the customer's card from the web page. Figure 9 shows an web page that might be used by the customer to select the ATM system and to enter the PIN number. The merchant would have a similar form with the account number and without the PIN number. In cases where the user has a card not supported by the ATM or point of sale system, extra charges may be incurred when performing transactions with a card that does not belong to the preferred system of the ATM or point of sale system. For example, one card may be a member of Exchange, Plus, Interlink and CU Access. Another Debit card may be configured as a member of Honor, Interlink, and Cirrus.

Generic card readers at merchant locations are configured to read from any type of card. Visa and Mastercard for example, may perform analysis of the card to determine which financial institution holds the account and additionally determines the type of account. The verification system of the present invention may keep a database of card number to bank account number conversions to allow the verification system to bypass the processing steps on the Visa/MC network and go straight to the ATM backbone further reducing transaction costs to the system. For example, only the first time a customer used the verification system would the system go through the Visa, Mastercard clearinghouse. This could reduce the costs of transactions even further, enhancing profit margin or lowering costs to merchants or customers.

In the preferred embodiment, the user interface displayed on the customer's web browser upon redirect to the verification system comprises navigational buttons to allow the user to return to the merchant prior to completion of the transaction. The interface may have the icons for the various debit service ATM backbones, as shown in Figure 8 and 9, where the user may select the appropriate symbol for the transaction such that the transaction is completed with the best transaction rate for that card. If the user selects an incorrect icon or if the debit card is not supported by the system the user is informed that the transaction cannot be completed with this card. The customer may be permitted to enter another card number and account at this time if the user wishes to proceed with this transaction. The system will be able to reconcile a change in the card selected since the verification number and transaction id are part of the current transaction. This will cause an update of the record stored in the database that was received by the TVS from the merchant.

If a user enters credit information into the debit field by mistake, the risk to the merchant is that someone really wanted to use a credit card. The system would be configured such that excess capability was available to serve our pages, and the interface would provide an easy mechanism for a user to backup to the merchant page to change the information entered to the correct field. One benefit might be that the user has now realized that the debit option is available and might change the card used for the purchase.

The following steps describe the process of purchasing via an Internet connection in more detail.

1. The customer goes to merchant's web page and decides to buy something. On the https:// page where they would normally enter a credit card, there is also an option for a Debit/Check card. The customer enters their card number,

and clicks the purchase button (buy it, whatever, just like they do now).

2. Because it is a Debit Card purchase, the merchant establishes a communications channel with the verification system and sends the card number, merchant ID, and the transaction amount.

3. The verification system returns to the merchant a data block containing a session ID, and verification information.

4. The merchant redirects the customer's web browser to the verification system server, passing the transaction ID as part of the address.

5.The verification system looks up the transaction information corresponding to the transaction ID, and presents a page to the customer requesting the information to complete the transaction, such as the PIN number and optionally the symbol representing the ATM backbone processing network, and/or other information from the card.

6. The verification system forwards the combined transaction information to the ATM backbone for completion of the transaction.

7. The verification system gets verification / approval from the backbone.

8. The customer is redirected back to the merchant web site, passing the expected verification block to the merchant as part of the address.

9. The merchant compares the verification block to the one received during the initial communication with the verification system, and if they match, knows that the transaction was successful.

In this mode of operation, the merchant never gets the pin. The verification system is the trusted third party and performs the communications with the financial backbone networks.

Optionally, software may be installed on the customer's machine and run locally that will retrieve customer information such as the PIN, and then using further cryptography techniques, pass that information to the verification system.

The system of the present invention may also be used for credit card processes or any other type of transaction where a third party (the verification server) holds part of the transaction information. For example, where the expiration date is held by the verification server for credit card transactions. Another example would be where a portion of a prepaid debit card may be provided to a third party, such that when the card is used at a merchant location, only part of the account number is known to the merchant. The customer would provide the remainder of the account number during the verification of the second part of the transaction with the customer.

The system may be used for the monthly billing transactions for insurance companies, gas credit cards, phone bills (bells and cellular), even email from your cellphone provider. For example, your Cell-phone bill for the month of March has been mailed to address which has a link provided to the system of the present invention such as "Try our Online Direct Check payment service by going to http://address…".

In another embodiment of the present invention, a functionality for check processing may be provided by the system. The backend for the present verification system is also capable of doing a new Automated ClearingHouse (ACH) funds transfer process. By getting the bank routing number and account number off of a check, funds can be transferred from the customer's account do operate with checks without requiring a printed check. Some merchants currently use a process where they may handle electronic payment by check but they are actually waiting for a real check. The processing costs associated with handling paper in this way could exceed that of credit cards. By utilizing the ACH/Direct Check method from the verification server, they could significantly reduce this cost, as well as offering another payment option to entice their customers. This is by far the cheapest option in terms of transaction costs. For an insurance company, it is actually cheaper than handling paper checks.

An additional feature of the system may incorporate an escrow option. The money for a transaction may be held in the verification system escrow account for a specified number of days and/or the customer must confirm receiving the goods before the money is released to the merchant's account.

System Advantages

- the merchant never gets the PIN number.
- the information to complete a transaction can never be intercepted by "eavesdropping" on any one channel of the communications between customer, merchant, or verification system.

- the verification system is trusted because the verification system conforms to the requirements of the different backbone processors.

- the net address of both the merchant and the customer may be held for use in fraud cases, however, the verification system would not be a party to the transaction done on behalf of the merchant.

Other Benefits Of The System

Many debit cards are also associated with major credit card companies in such a way that they can also be used as credit cards. We can enhance the security of using these cards for debit card transactions, by requiring that the merchant NOT request the card expiration date, thus minimizing the possibility that the debit card can be used in an unauthorized credit card transaction. This makes the cards more easily managed and more secure than typical credit card transactions. For example, a merchant cannot make an unauthorized credit card transaction without the expiration date. For debit card transactions this date is not required, instead the customer is the only person with enough information to respond to the query for the PIN number. The merchant never has the pieces to do a debit transaction without the user entering the pin on the verification server site.

Internet merchants are paying 2.2 to 6% to a clearinghouse organization to take credit cards over the Internet. This is referred to as the non-swiped rate (the card is not physically available to run through a terminal.) The rate is higher due to the potential for fraud. Because the present system will be able to provide the PIN number, therefore proving to a greater extent that the customer is in actual possession of the card, a more favorable processing rate can be negotiated. The system of the present invention can therefore give the merchant the chance to decrease their transaction costs.

The verification system subscribers such as preferred merchants would benefit greatly from making the distinction up front between debit and credit cards. For example, one potential customer uses a typical order page that looks like the sample shown in Figure 5. By changing the page to include a debit card field, the transactions form would look more like Figure 6. Based on the preferential physical placement of the debit card information, it would be more likely that a customer would choose the debit option. The user may benefit if part of the cost savings are passed onto them and the merchant would see a reduction in transaction costs.

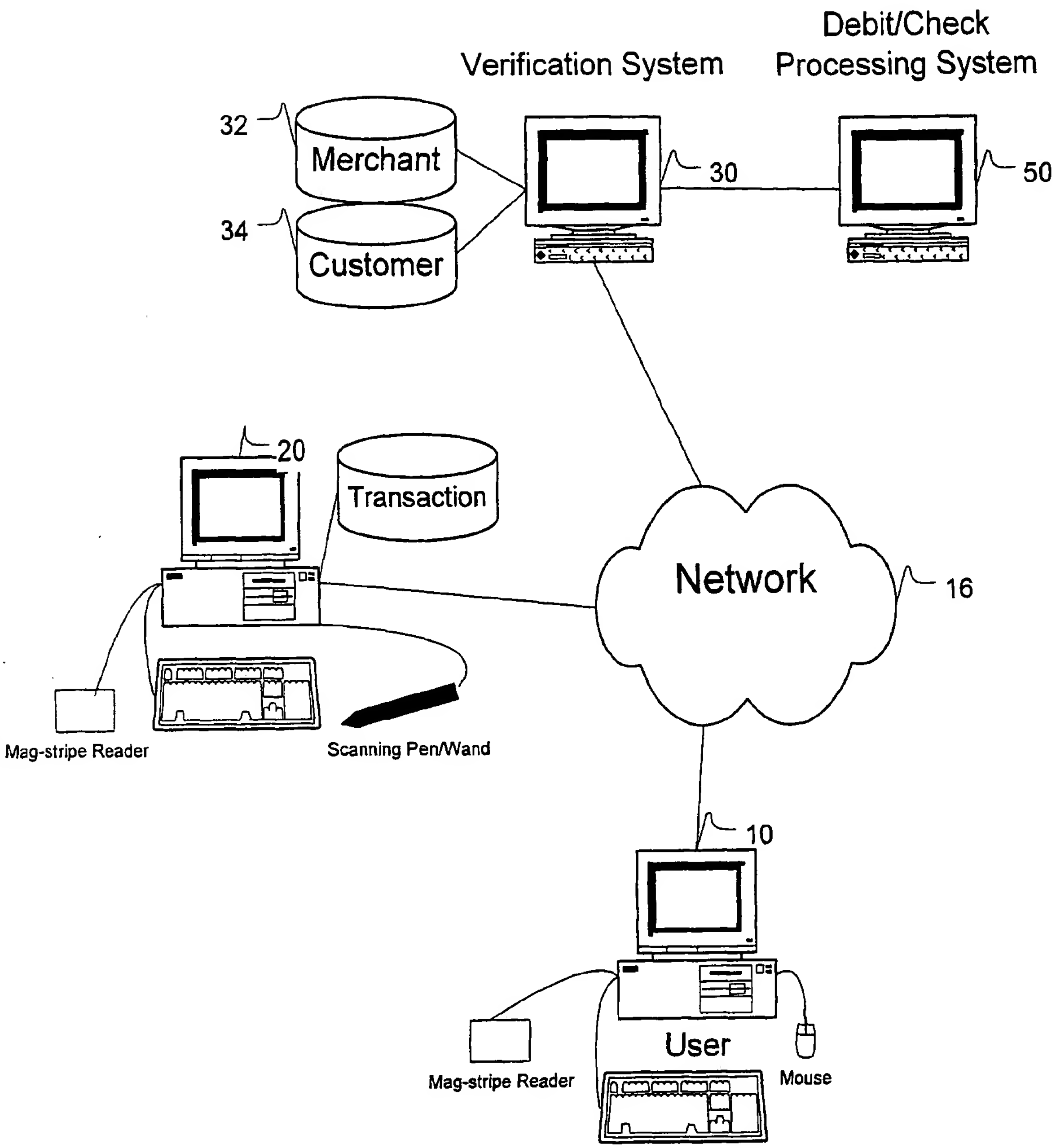


Figure 1

Docket No
700-198P
Sheet 1 of 6

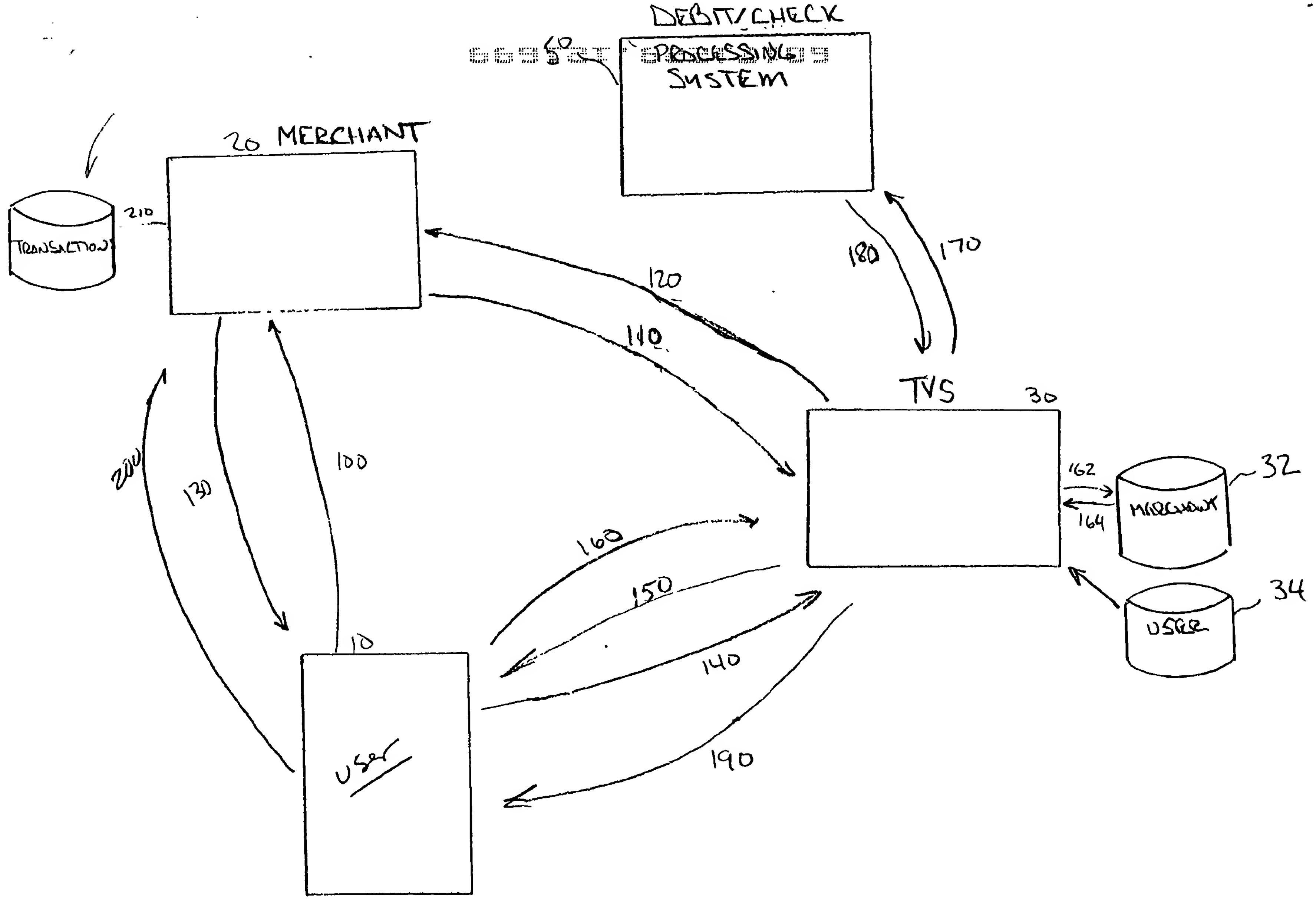


Figure 2

DOCKET NO
700-198P
SHEET 2 OF 6

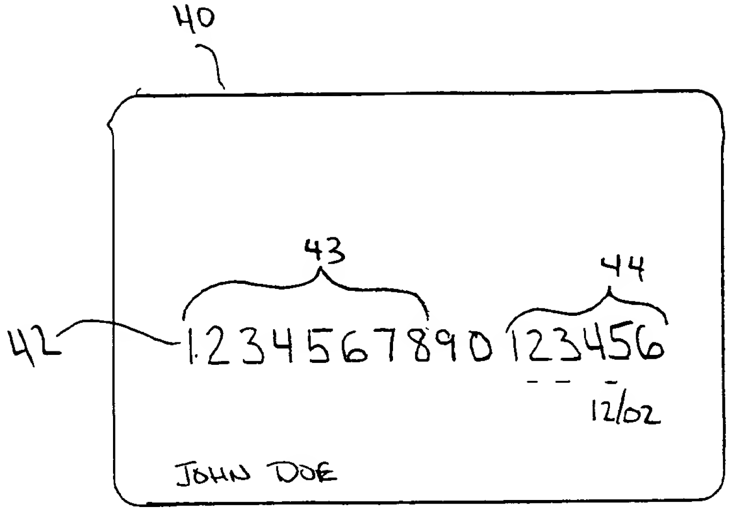


FIGURE 3

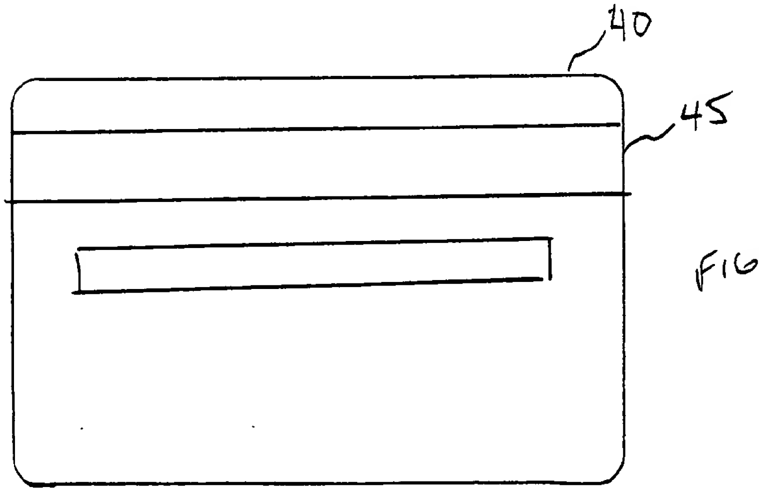
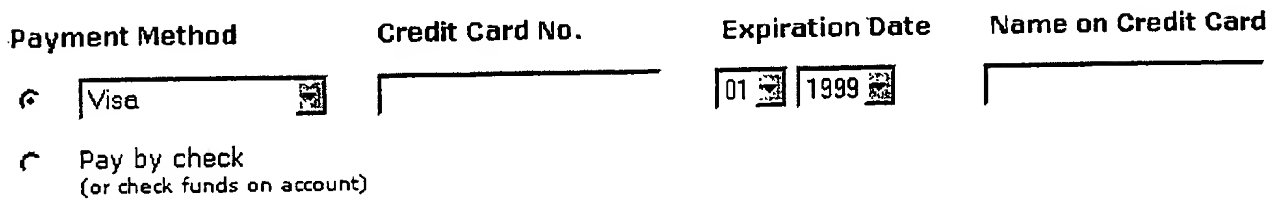


FIGURE 4

DOCKET NO
700-198P
SHEET 3 OF 6



Payment Method

● Visa

○ Pay by check
(or check funds on account)

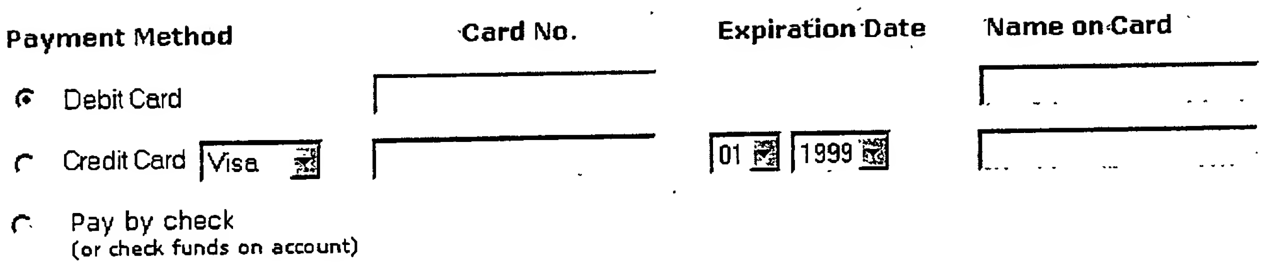
Credit Card No.

Expiration Date

01 1999

Name on Credit Card

Figure 5



Payment Method

● Debit Card

○ Credit Card Visa

○ Pay by check
(or check funds on account)

Card No.

Expiration Date

01 1999

Name on Card

Figure 6

DOCKET NO
700-198P
SHEET 4 OF 6

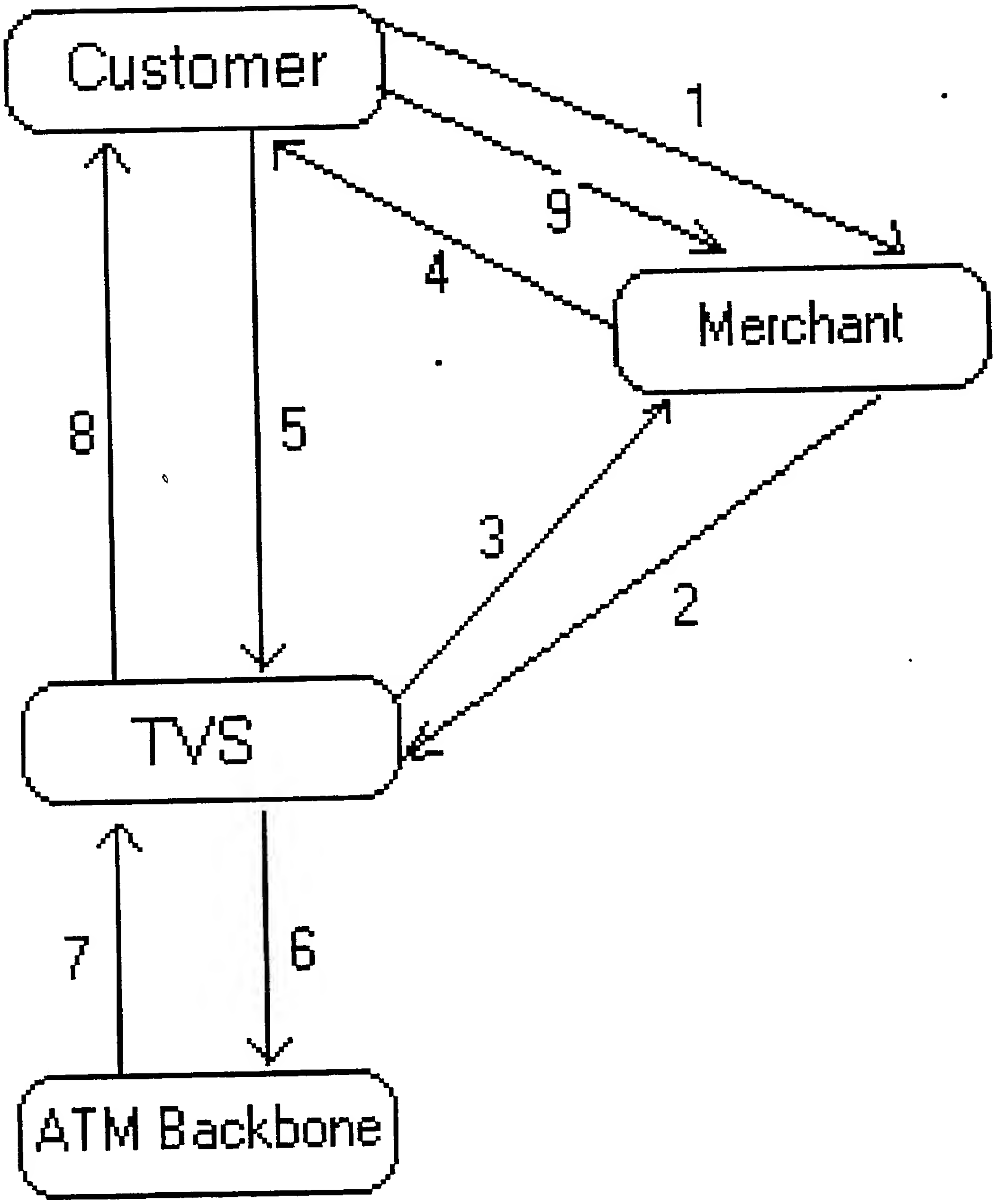
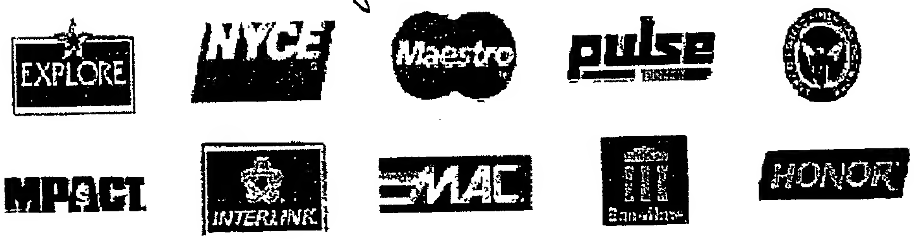
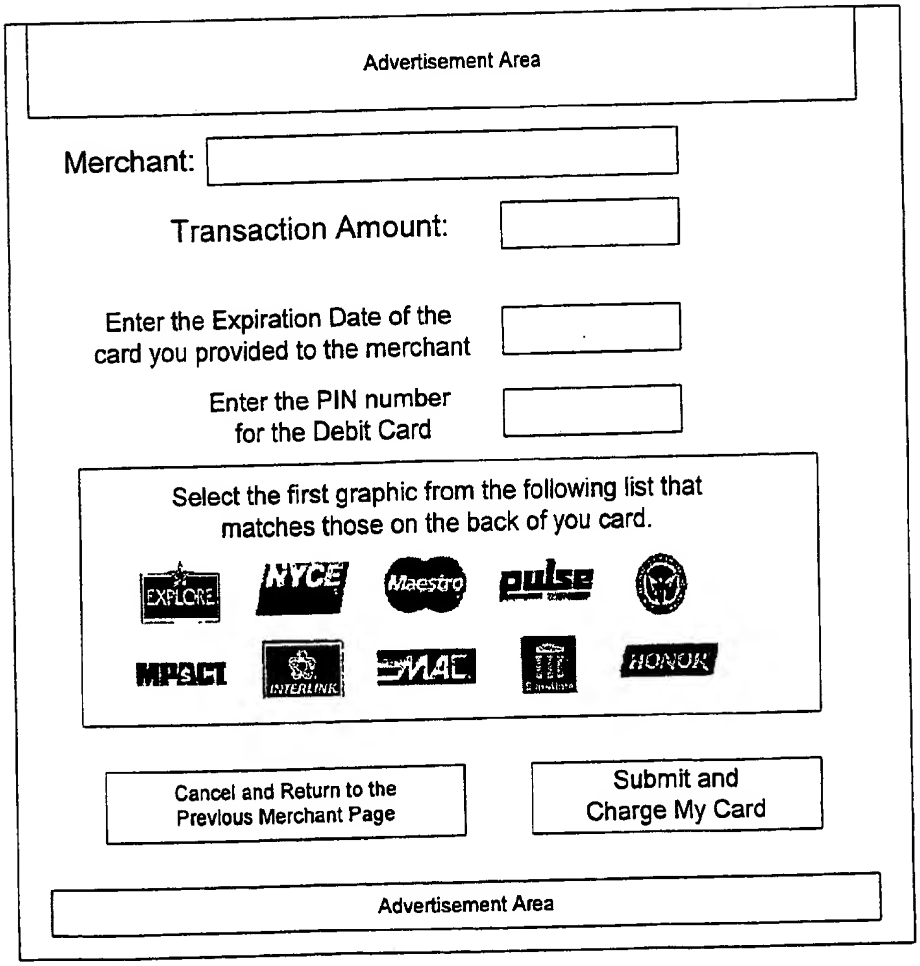


Figure 7

DOCKET NO
700-198P
SHEET 5 OF 6

Figure 8





Merchant:

Transaction Amount:

Enter the Expiration Date of the card you provided to the merchant

Enter the PIN number for the Debit Card

Select the first graphic from the following list that matches those on the back of you card.

EXPLORE
NYCE
Maestro
pulse
MPACT
INTERLINK
MAC
HONOR
Cancel and Return to the Previous Merchant Page
Submit and Charge My Card
Advertisement Area

Figure 9

DOCKET NO
700-198P
SHEET 6 OF 6